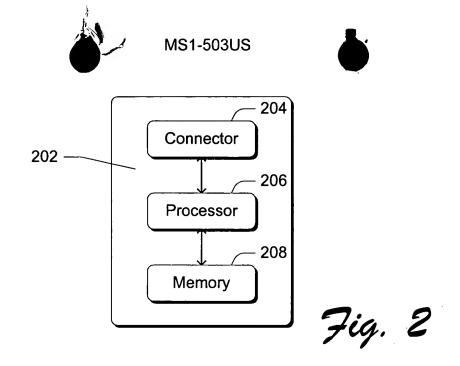
١



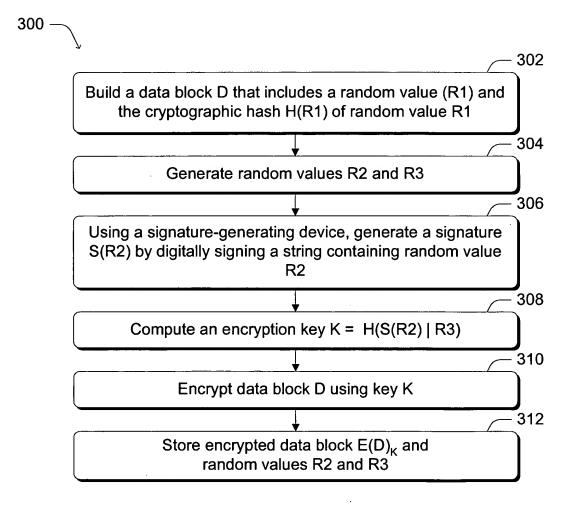


Fig. 3



400 -



Access stored encrypted data block E(D)_k and

404

402

Using a signature-generating device, generate a signature TS(R2) by digitally signing a string containing a stored random value R2

random values R2 and R3

406

Compute an decryption key TK = H(TS(R2) | R3)

408

 $\mathsf{Decrypt}\;\mathsf{E(D)}_{\mathsf{K}}\;\mathsf{using}\;\mathsf{TK}$

- 410

Generate a cryptographic hash of the recovered random number R1 (from decrypted data block D) and compare it with the recovered H(R1) within decrypted data block D

Fig. 4